

Welcome to:

Project Broadsword

Broadsword

Version 3.0
Security Log's
Training Guide

Broadsword Program Office
Air Force Research Laboratory /
315-330-4429

How do I query for information user ?

Audit Log Maintenance	
User :	<input type="text"/>
Start Date :	YYYYMMDDhhmmss <input type="text" value="20000628202053"/>
End Date :	YYYYMMDDhhmmss <input type="text" value="20000628202053"/>
Event :	<input type="text" value="All Events"/>
Archive File Name :	<input type="text"/>

Audit Report Archive Records Remove

What types of information query for?

Session Searching Cataloging Administration ISSO Help

Audit Log Maintenance

User : bilinski

Start Date : YYYYMMDDhhmmss
20000629115929

End Date : YYYYMMDDhhmmss
20000629115929

Event : All Events

Archive File Name :

- All Events
- Added DAC
- Added Group
- Modified Group
- Added Group Member
- Removed Group
- Removed Group Member
- Added New Source
- Get Column Attributes
- Added User Privileges
- Audit Dump

Audit Report Archive Records Remove Records

How do I generate an Audit Re

Session Searching Cataloging Administration ISSO Help

Audit Log Maintenance

User :	bilinski
Start Date :	YYYYMMDDhhmmss 20000629115929
End Date :	YYYYMMDDhhmmss 20000629115929
Event :	User Logged In
Archive File Name :	

Audit Report Archive Records Remove Records

How do I view the Audit Report

Session Searching Cataloging Administration ISSO Help

Audit Log Maintenance

User : bilinski

Start Date : YYYYMMDDhhmmss
20000629115925

End Date : YYYYMMDDhhmmss
20000629115925

Event : User Logged In

Archive File Name :

[View Audit Report](#)

Audit Report Archive Records Remove Records

What does my Audit Report look like?

This is the report header. It contains all of the audit log criteria specified in the previous screen.

Audit Report

User: bilinski for All Dates For User Logged In

Login: bilinski **IP:** 255.255.255.255 **Origin:** bilinski **Gitpr:** 255.255.255.255 **Session Keys:** 1212
 LOGIN @ 255.255.255.255 : Successful Login from maleph Gatekeeper
Login: bilinski **IP:** 255.255.255.255 **Origin:** bilinski **Gitpr:** 255.255.255.255 **Session Keys:** 1212
 LOGIN @ 255.255.255.255 : Successful Login from maleph Gatekeeper
Login: bilinski **IP:** 255.255.255.255 **Origin:** bilinski **Gitpr:** 255.255.255.255 **Session Keys:** 1212
 LOGOUT 255.255.255.255 : Gatekeeper timed out from Gatekeeper

This is a sample log entry. Each entry contains the username, IP Address, Gatekeeper, and Session Key, as well as all of the events that were audited

How do I Archive a Report?

Session Searching Cataloging Administration ISSO Help

Audit Log Maintenance

User : bilinski

Start Date : YYYYMMDDhhmmss
20000629115929

End Date : YYYYMMDDhhmmss
20000629115929

Event : User Logged In

Archive File Name : audittest

Archived record(s) successfully.

Audit Report Archive Records Remove Records

How do I remove a Record

Session Searching Cataloging Administration ISSO Help

Audit Log Maintenance

User : bilinski

Start Date : YYYYMMDDhhmmss
20000710130905

End Date : YYYYMMDDhhmmss
20000710130905

Event : User Logged In

Archive File Name : audittest

**WARNING: Verify Record Deletion by Clicking Remove Records Again.
These Records will be PERMANENTLY Removed from the System.**

Audit Report Archive Records Remove Records

Where are the files I have Archived?

Session Searching Cataloging Administration ISSO Help

Audit Archive Queries

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input type="checkbox"/>	test08adduser	20000629132908
<input checked="" type="checkbox"/>	bilinski1	20000629152333
<input type="checkbox"/>	all_test02_62900	20000629165051
<input type="checkbox"/>	audit050599	20000629170856
<input type="checkbox"/>	security_test	20000629172911

User : bilinski1

Start Date : YYYYMMDDhhmmss
20000629115929

End Date : YYYYMMDDhhmmss
20000629115929

Event : User Logged In

Query Archives

Local intranet zone

Where are the files I have Archived continued..

Session Searching Cataloging Administration ISSO Help

Audit Archive Queries

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input type="checkbox"/>	test08adduser	20000629132908
<input type="checkbox"/>	bilinski1	20000629152333
<input type="checkbox"/>	all_test02_62900	20000629165851
<input type="checkbox"/>	audit050599	20000629170856
<input type="checkbox"/>	security_test	20000629172911
<input type="checkbox"/>	auditbilinski	20000710141602
<input type="checkbox"/>	audittest	20000710145515

User :

Start Date :

End Date :

Event :

[View Audit Report](#)

Query Archives